1 - BCTAA Employee Device Access

Appropriateness of Protection Measure

It is an important consideration that each employee at BCTAA is able to keep their own work safe and secure, where only they can access it.

Alternative Protection Measures that Could be Used

Alternatively, each computer at the office could be unique to the employee that uses it, meaning that only person A can use computer A and so on. This would mean that every user logs in to their own allocated computer to manage their own files.

A downside to the idea of having individual PCs for each employee, would be that they wouldn't be networked together, meaning that there would be no way for them to share files directly over the network.

Rationale for Choice of Protection Measure

The reason I chose this protection measure was so that employees are able to securely store and access the files that relate to their jobs, while still being able to share files and to access publically shared files.

2 - Theft or Copying of Door Access Card

Appropriateness of Protection Measure

It is important to educate the employees of the risks that can exist when they do not look after their access cards, because it will promote them to keep their cards safe and to not allow them to be used by others.

It is also an important step to increase the security regarding the card-based access to the office, so that the office is kept physically secure.

Alternative Protection Measures that Could be Used

An entirely different access method could be employed, like a keycode that all employees must memorise, or a biometric fingerprint scanner that all employees have been whitelisted on.

The issues with these come down to the expense of biometrics and technical proficiency required to set it up and maintain it, as well as the possibility of misremembering a code for a keypad as the code will likely change on a regular basis.

Rationale for Choice of Protection Measure

I think that the best method for protecting cards is to keep employees aware of the security risks, to improve the physical security that protects physical access, and to provide capabilities of preventing card ID theft such as RFID proof wallets.

3 - Man in the Middle Attack

Appropriateness of Protection Measure

I believe that the protection measure of ensuring that all wireless communication is encrypted is very appropriate for BCTAA. In order to prevent attackers from being able to intercept and then read sensitive information passed via a wireless transmission, the data being sent must be encrypted. Failure to ensure encryption would resort in untrustworthy wireless communication.

Alternative Protection Measures that Could be Used

An alternative to risking data and information that is being sent to, from, and within the network, would be to use wired connections for as much communication as possible. This would be impossible to achieve between the network and the internet/client, but BCTAA could cut down on any of the wireless devices that are being used, and replace them with wired connections. For example, the staff mobile devices would not be allowed to connect to the network.

Rationale for Choice of Protection Measure

I believe that the protection measure I have come up with is vital if wireless communication is to be had with the EH network. Therefore, wireless encryption via protocols such as FTP or TLS is required.

4 - Public Areas Hours

Appropriateness of Protection Measure

The accessibility to both, the EH network, and the building itself by guests is possible outside of the typical working hours of the offices at the building, meaning that the offices of the network are potentially more at risk, since they are empty of employees, unsupervised, which could allow an attacker to gain access.

It is therefore important to ensure additional measures of security to lessen the risk of unauthorised access to the office, or to the network.

Alternative Protection Measures that Could be Used

The network in its entirety could be blocked after certain hours, or the building's services could be only opened during certain hours, as a way of protecting the employees.

This would be impractical though, because the other businesses, such as the restaurant and art gallery would not benefit from this restriction.

Rationale for Choice of Protection Measure

The reason that I have chosen to support the methods of protecting the system, is that they are potentially practical and realistic. The 19th floor could be inaccessible at certain times, security staff could be hired, and CCTV will definitely be in place in and around the office.

5 - Physical Access to Devices

Appropriateness of Protection Measure

Using physical security to protect sensitive data and information that is kept on the system, is a necessary procedure. If unauthorised people do gain access to the office, despite the access card system, they mustn't be able to access the devices within, since that would give them access to personal data and private information.

Alternative Protection Measures that Could be Used

Sensitive information could be kept elsewhere so that it cannot be stolen if access is gained to the office.

This would be useful in terms of data and information protection but would be impractical in some ways, since BCTAA would be relying on a third party to keep the data safe.

Rationale for Choice of Protection Measure

Using locks and passwords to protect devices are important considerations when it comes to protecting data, and is a vital requirement on top of the digital security that is in place.

6 - Harmful Use of System

Appropriateness of Protection Measure

Steps must be taken to protect the network from being used it harmful ways, a firewall is the most efficient tool that can be used on a network to protect that network from undesirable actions.

Alternative Protection Measures that Could be Used

Employees could be educated and informed of the risks of browsing the internet, sharing information, and correctly securing data. Policies could be put in place to restrict certain behaviour and actions online.

Employees are still capable of making mistakes however, and without the restriction from a firewall, this is very likely.

Rationale for Choice of Protection Measure

A firewall is the best way of controlling the way that a network is used, since it is able to meet the requirements of the business while still keeping it safe from any outside threats.

7 - Risk of Virus

Appropriateness of Protection Measure

The instalment of software that aims to locate and remove harmful software, is a must for BCTAA. Antivirus software and other software that protect devices from harm, are very important when files are being shared, email is being used, and downloads happen within a business.

Additionally, web filters are another necessary feature that protect the devices of a network against malicious content.

Alternative Protection Measures that Could be Used

Without the security that is provided by web filters and antimalware software, devices at the network are at risk of getting a virus. All it takes is for one untrustworthy email attachment to be downloaded, and the entire network is at risk of the virus.

Rationale for Choice of Protection Measure

Viruses must be protected against, as must other kinds of malware. Without software to detect and remove malware on each device of a network, the network is at risk.

8 - Visitors and Employees Sharing a Switch

Appropriateness of Protection Measure

BCTAA must ensure that visitors are unable to access employee files on the network, and the best way to ensure this is to employ separate VLANs on the switch that they both use.

Alternative Protection Measures that Could be Used

A different switch could be used altogether for visitors to connect to, but this would require additional costs and changes to the infrastructure of the network.

Rationale for Choice of Protection Measure

It is important that the devices used by employees, and the devices used by visitors are kept separate, so that there is no risk of visitors gaining access to employee content on the network. That could lead to theft or loss of data and information that is vital for BCTAA.